Mayhem – malware za vaše Linux i BSD servere

Virus Bulletin donosi zanimljiv poduži opis malware aplikacije nazvane Mayhem [1]. Najprije dobre vijesti: iako ovaj malware napada i Linux i BSD servere, za uspješan napad nužno je ispuniti neke preduvjete koje dobro održavani serveri uglavnom nemaju: dozvolu za upload php datoteka i njihovo izvršavanje na lokalnom računalu, a i php.ini mora specifično dozvoljavati *system()* i *exec()* pozive, što po defaultu nije slučaj (ili imate jako, jako staru verziju PHP-a).

Ako smo apsolvirali taj aspekti sigurnosti sustava, možemo pročitati i kako malware radi.

Po infekciji, malware instalira PHP skriptu čija je svrha detektirati na kojem OS-u radi (Linux ili BSD), te vrti li se na 32- ili 64-bitnom sustavu. Potom malware ubija host procese i kreira *libworker.so* datoteku u kojoj se nalazi maliciozni *payload* u mašinskom kodu. Sljedeći korak je instalacija bash skripte i njeno pokretanje kao *cron* joba koji pokreće maliciozni binarni *payload* koji se nalazi u .so datoteci. To čini je korištenjem LD_PRELOAD direktive kojom se li*bworker.so* "nalijepi" na naredbu /usr/bin/host (ali je ne mijenja) kako bi se maliciozni kod mogao izvršiti uz normalnu funkcionalnost naredbe.

Što se nakon toga događa postaje malo kompleksnije, pa preporučujemo da pročitate članak Virus Bulletina, a nama je zanimljivo samo spomenuti kako se zaraženi server pridružuje botnetu i čeka naredbe C&C centra (u članku su opisane i C&C naredbe), kako uredno (ali limitirano) funkcionira i bez dobivanja root privilegija, te kako su pisci malicioznog softvera predvidjeli i mogućnost povlačenja i izvršavanja plug-in skripti kroz C&C mrežu. Podatke i konfiguraciju ovaj malware sprema u skriveni datotečni sustav, u naravi datoteku sa točkom na početku imena koja služi kao virtualni disk i sadrži modificirani FAT datotečni sustav zaštićen enkripcijom.

Sumnjate li na mogućnost zaraze, ovo su koraci koje možete poduzeti:

1. provjerite postojanje inicijalne PHP skripte (pretražite uobičajene upload direktorije) čiji SHA256 hash je b3cc1aa3259cd934f56937e6371f270c23edf96d2c0801 728b0379dd07a0a035;

2. provjerite koristi li neka skripta u dosegu apache/php procesa varijablu "AU" koja sadrži URL do maliciozne skripte;

3. ako ste posebno paranoidni, zabranite običnim korisnicima korištenje *cron* usluge;

4. najzad, čini se kako su autori zaboravili počistiti PHP kod, pa se malware neće izvršiti ako imate postavljenu varijablu MAYHEM_DEBUG.

ned, 2014-07-20 07:48 - Radoslav Dejanović**Vijesti:** Sigurnost [2]
Vote: 0

No votes yet

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

Source URL: https://sysportal.carnet.hr./node/1419

Links
[1] https://www.virusbulletin.com/virusbulletin/2014/07/mayhem-hidden-threat-nix-web-servers
[2] https://sysportal.carnet.hr./taxonomy/term/13

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr